pour tout entier a et pour tout entier b non nul , il existe un couple unique d'entiers (q , r) tel que

$a = bq + r$ et $0 \leq r \leq |b|$.

Le reste de tout entier n dans la division euclidienne par un entier non nul b est un élément de l'ensemble $\{ 0 , 1 , 2 , ... , \leq |b| - 1 \}$.

Congruence

Soit n un entier naturel et non nul et a et b deux entiers .

1°/On dit que a est congru à b modulo n (ou a et b sont congrus modulo n) si a – b est un multiple de n . on note alors $a \equiv b \pmod n$.

2°/ Soit n un entier naturel non nul .

Pour tout entier a , il existe un unique entier r appartenant à $\{ 0 , ..., n - 1\}$ tel que $a \equiv r \pmod n$. On dit que r est le reste modulo n de a .

3°/Soit n un entier naturel non nul .

Deux entiers sont congrus modulo n , si et seulement si , ils ont le même reste modulo n .

4°/Soit a , b et c trois entiers et n un entier naturel non nul .

$a \equiv a \pmod n$

Si $a \equiv b \pmod n$ alors $b \equiv a \pmod n$

Si $a \equiv b \pmod n$ et $b \equiv c \pmod n$, alors $a \equiv c \pmod n$.

5°/Soit a , b , c et d quatre entiers et n un entier naturel non nul .

Si $a \equiv b \pmod n$ et si $c \equiv d \pmod n$, alors

$a + c \equiv b + d \pmod n$ et $a \times c \equiv b \times d \pmod n$.

Si $a \equiv b \pmod n$ alors $ha \equiv hb \pmod n$ pour tout entier h et $am \equiv bm \pmod n$ pour tout entier $m > 0$.